BRL

TECHNICAL NOTE NO. 1113
FEBRUARY 1957

SUMMARY DISCUSSION ON PERFORMING BINARY MULTIPLICATION WITH THE FEWEST POSSIBLE ADDITIONS

George W. Reitwiesner

Department of the Army Project No. 5B0306002
Ordnance Research and Development Project No. TB3-0007

BALLISTIC RESEARCH LABORATORIES

ABERDEEN PROVING GROUND, MARYLAND

B A L L I S T I C   R E S E A R C H   L A B O R A T O R I E S

TECHNICAL NOTE NO. 1113

FEBRUARY 1957

SUMMARY DISCUSSION
ON PERFORMING BINARY MULTIPLICATION
WITH THE FEWEST POSSIBLE ADDITIONS

George W. Reitwiesner

Department of the Army Project No.5B0306002
Ordnance Research and Development Project No. TB3-0007

A B E R D E E N   P R O V I N G   G R O U N D,   M A R Y L A N D

B A L L I S T I C   R E S E A R C H   L A B O R A T O R I E S

TECHNICAL NOTE NO. 1113

GWReitwiesner/blf
Aberdeen Proving Ground, Md.
February 1957

SUMMARY DISCUSSION ON PERFORMING BINARY MULTIPLICATION WITH THE FEWEST POSSIBLE ADDITIONS

ABSTRACT

Under conventional binary multiplication procedures an addition (or, equivalently, a subtraction) is performed for each non-zero digit of the multiplier or its absolute value, and the statistically expected number of additions per multiplication is one-half the number of these digits.

This discussion develops Boolean functions for the recursive definition of substitute sets of multiplier digits, for which the numbers of non-zeros are irreducible with statistically expected values very near one-third the number of digits which express the signed multiplier, and applies these functions to the three known binary representations: 2's complement, 1's complement, and magnitude with appended sign.

PREFACE

This note summarizes briefly a formal study which was begun early in January 1957 and for which the draft of a formal report was completed on 23 January 1957.

This note is essentially a draft of a proposed talk of approximately one-quarter hour duration which is intended for presentation at the June 1957 meeting of the Association for Computing Machinery.

Conventionally, binary multiplication is performed by recursively executed shifts of an intermediate product, interspersed with additions or subtractions. The choice between whether or not an addition or subtraction is performed is governed by which of two values, 0 or 1, is held by each momentarily examined digit of the multiplier, and the choice between adding and subtracting is governed by considerations of number representation and multiplier sign.

This discussion briefly summarizes a rigorous and more lengthy argument which derives for each of the three known representations for binary data (2's complement, 1's complement, and magnitude with appended sign) a set of replacement multiplier digits which admit the three values -1, 0, and +1 and for which the number of non-zeros is irreducible.

Immediately apparent is the application to performing binary multiplication with the fewest possible additions and subtractions, and hence in minimum time, but there exists the significant reservation that this discussion is not concerned with reducing the number of required shifts, nor with possible interplay of shifting action with addition and subtraction.

Throughout this discussion the three-valued digits are referred to as "coefficients" to distinguish them from two-valued "digits".

That the coefficients admit three values introduces, per se, no serious design problem, for the association of sign with any coefficient, or with the entire multiplier itself, corresponds simply to a selection between adding and subtracting during the multiplication process.

Throughout this discussion the multiplier is considered to be an integer. This is done strictly for notational convenience. It is not inconsistent with conventional scaling of data to lie in the range from -1 to +1, for shifting the radix point has no effect upon the values held by the individual coefficients or digits.

Initially this discussion is concerned with non-negative integer multipliers A_n and B_n which are defined in Fig. 1 in terms of n+1 digits a_i and coefficients b_i and which are restricted to lie in the exhibited ranges, whence the highest indexed digit and the two highest indexed coefficients are restricted in their values as shown.

Since the sets of coefficients which define two integers of equal magnitude and opposite sign are related to each other simply by the inversion of the signs of the non-zeros, no loss of generality of application is occasioned by restricting the argument initially to non-negative multipliers; and since the limiting index n is arbitrary, the range restrictions also occasion no loss of generality.

Ultimately, for each of the three representations, the limiting index n will be related to the number of digits by which the signed multiplier is defined, and the a's will be related to the non-sign multiplier digits, with the apparent vacancy in the digit $a_n = 0$ being filled by the sign of the multiplier.

$$A_n = \sum_0^n a_i . 2^i \qquad a_i = 0, 1.$$

$$B_n = \sum_0^n b_i . 2^i \qquad b_i = -1, 0, +1.$$

$$0 \leqq A_n \leqq 2^n - 1 \implies a_n = 0.$$

$$0 \leqq B_n \leqq 2^n - 1 \implies \begin{cases} (b_n)(b_{n-1}) = 0. \\ b_n \neq -1 \neq b_{n-1}. \end{cases}$$

Fig. 1.

The argument begins with the demonstration of the procedure for replacing the a's with the b's.

The replacement is accomplished through the identity exhibited in Fig. 2 for arbitrary limiting index α and is illustrated in the example shown for a particular integer $A_{16} = B_{16}$. Superscoring denotes a negative coefficient.

The procedure is simply that of repeatedly applying the identity to the lowest indexed chain of two or more consecutive non-zeros until it no longer can be applied.

In the example, the identity is first applied to the chain a_2, a_3, yielding $b_2 = -1$ and $b_4 = +1$; next it is applied to the chain a_7, a_8, yielding $b_7 = -1$ and $b_9 = +1$; it is significant that b_9 then combines with a_{10} and a_{11} to form the next chain affected, and here the identity reverses the sign of b_9 and yields $b_{12} = +1$; finally the chain a_{14}, a_{15} yields $b_{14} = -1$ and $b_{16} = +1$.

The properties of the resulting set of b's are: (1) no two consecutively indexed b's are both non-zero; (2) they are uniquely determined; (3) they contain the minimum possible number of non-zeros; (4) they are recursively definable from knowledge essentially only of the a's; and (5) if each a assumes the values 0 and 1 with independent probability 1/2, then the expected number of non-zero b's is very close to $(n+1)/3$.

$$2^{\alpha} + \dots + 2^2 + 2^1 + 2^0 = 2^{\alpha+1} - 1.$$

	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
A_{16} =	0	1	1	0	0	1	1	0	1	1	0	0	0	1	1	0	1
B_{16} =	1	0	$\bar{1}$	0	1	0	0	$\bar{1}$	0	$\bar{1}$	0	0	1	0	$\bar{1}$	0	1

Fig. 2.

In Fig. 3 the replacement procedure is exhibited in formal terms: Here are the functions by which the b's are recursively defined in terms of essentially only the a's. The quantities λ and γ are transition parameters which admit the values 0 and 1 and, commencing with the initial conditions shown, carry the recursion through consecutively increasing values of the index j. Indeed, γ_j is the absolute value of the coefficient b_j, and the sign of b_j is fixed by the factor $(1 - 2a_{j+1})$. The stipulation $a_{n+1} = 0$ is trivially necessary to provide the proper sign for b_n.

$$\left.\begin{aligned}
\lambda_{j+1} &= a_j (\lambda_j + \gamma_{j-1}) \\
\gamma_j &= (1 - \gamma_{j-1}) \left[(1 - a_j)\, \lambda_j + (1 - \lambda_j)\, a_j \right] \\
b_j &= (1 - 2a_{j+1})\, \gamma_j
\end{aligned}\right\} \quad j = 0, 1, \ldots n.$$

$$\lambda_0 = \gamma_{-1} = 0.$$

$$a_{n+1} = 0.$$

Fig. 3.

2^j-1		H_j		A_j		a_j j=543210	b_5	b_4	b_3	b_2	b_1	b_0
2^0-1	=	H_0	=	0	=	000000						
2^1-1	=	H_1	=	1	=	000001						1
		H_2	=	2	=	000010					1	
2^2-1	=			3	=	000011				1		-1
				4	=	000100				1		
		H_3	=	5	=	000101				1		1
				6	=	000110			1		-1	
2^3-1	=			7	=	000111			1			-1
				8	=	001000			1			
				9	=	001001			1			1
		H_4	=	10	=	001010			1		1	
				11	=	001011		1		-1		-1
				12	=	001100		1		-1		
				13	=	001101		1		-1		1
				14	=	001110		1			-1	
2^4-1	=			15	=	001111		1				-1
				16	=	010000		1				
				17	=	010001		1				1
				18	=	010010		1			1	
				19	=	010011		1		1		-1
				20	=	010100		1		1		
		H_5	=	21	=	010101		1		1		1
				22	=	010110	1		-1		-1	
				23	=	010111	1		-1			-1
				24	=	011000	1		-1			
				25	=	011001	1		-1			1
				26	=	011010	1		-1		1	
				27	=	011011	1			-1		-1
				28	=	011100	1			-1		
				29	=	011101	1			-1		1
				30	=	011110	1				-1	
2^5-1	=			31	=	011111	1					-1

Fig. 4

In concrete illustration there is exhibited in Fig. 4, for the particular case $n = 5$, the entire family of $2^5 = 32$ sets of b's which correspond to the $2^5 = 32$ possible sets of a's.

Clearly, the upper half of this figure exhibits the same illustration for $n = 4$; the upper quarter, for $n = 3$; and so on. And by analogy, the figure is extensible in the other direction to accommodate higher values of n.

The numbers H_j are defined by alternating digits 0 and 1 among the a's, and these arrays define the truncated binary fractions 1/3 and 2/3 when the radix point is located adjacent to a_j.

For $n = 5$ the coefficient b_5 has non-zero value for and only for the values of the integer A_5 which lie between H_5 and 2^5-1, and the coefficient b_4 has non-zero value for and only for the values of the integer A_5 which lie between H_4 and H_5. Except only for sign changes, the table repeats itself in halves, quarters, etc. for the succeeding lower indexed b's, and therefore the number of non-zeros for each of the b's is expressible as a function of the correspondingly indexed H's.

A corresponding argument applies for any n.

From the values of the numbers H_j (approximately 1/3 and 2/3 when the radix point is located adjacent to a_j), the number of non-zeros for each of the b's is close to $2^n/3$.

In Fig. 5 the exact number of non-zero coefficients for any index, j or n, is exhibited as P_j and P_n.

If each digit a_i assumes the values 0 and 1 with independent probability 1/2, then each of the 2^n possible combinations of values among the a's occurs with probability 2^{-n}, whence it follows that the expected numbers of non-zero b's whose indicies are less than or equal to a particular index, j or n, are given by E_j and E_n in this figure.

$$P_j = (2^n + (-1)^j.2^{n-1-j})/3 \qquad j \leqslant n$$

$$P_n = (2^{n-1} - 3 + (-1)^n)/6$$

$$E_j = \sum_0^j 2^{-n}.P_k = (j+1)/3 + (1 + (-1)^j.2^{-(j+1)})/9 \qquad j \leqslant n$$

$$E_n = \sum_0^n 2^{-n}.P_k = (n+1)/3 + (1 + (-1)^n.2^{-(n+1)})/9 - 2^{-(n+1)}$$

Fig. 5.

Toward applying the Boolean functions to the three number representations, there are exhibited in Fig. 6 the definitions and ranges of signed integers X_2, X_1, and X_A for the three respective representations: 2's complement, 1's complement, and magnitude with appended sign.

In all three cases the integer X is defined by an arbitrary number W of digits x_i which admit the two values 0 and 1, with the highest indexed digit indicating the sign of the integer: not less than zero if 0, and not greater than zero if 1. The sign of the integer zero is ambiguous only in the latter two mentioned representations.

It remains to apply the foregoing arguments by relating n to W and the a's to the x's.

$$X_A = (1 - 2x_{W-1}) \cdot \sum_0^{W-2} x_i \cdot 2^i$$

$$X_1 = \sum_0^{W-2} (x_i - x_{W-1}) \cdot 2^i$$

$$X_2 = -x_{W-1} \cdot 2^{W-1} + \sum_0^{W-2} x_i \cdot 2^i$$

$$0 \leq |X_A| < 2^{W-1}$$

$$0 \leq |X_1| < 2^{W-1}$$

$$-2^{W-1} \leq X_2 < 2^{W-1}$$

Fig. 6.

$$X_A = (1 - 2x_{W-1}) \cdot \sum_0^{W-2} x_i \cdot 2^i \qquad n = W-1$$

$$X_1 = \sum_0^{W-2} (x_i - x_{W-1}) \cdot 2^i \qquad n = W-1$$

$$= (1 - 2x_{W-1}) \cdot \sum_0^{W-2} \left[(1-x_i)x_{W-1} + (1-x_{W-1})x_i \right] 2^i$$

$$X_2 = -x_{W-1} \cdot 2^{W-1} + \sum_0^{W-2} x_i \cdot 2^i \qquad n = W$$

$$= -x_{W-1} \cdot 2^W + \sum_0^{W-1} x_i \cdot 2^i$$

Fig. 7.

In Fig. 7 the integer definitions are rephrased to forms more tractable for the application of the Boolean functions. For the 1's complement case X_1 is reexpressed as a signed magnitude, and for the 2's complement case X_2 is reexpressed to place the sign digit both inside and outside of the summation. Also the relationships between n and W are shown. It is momentarily significant that n is relatively one higher for the 2's complement case than for the other two cases.

In all cases the a's are defined as the respective coefficients of 2^i in the summations shown (the rephrased summations for both complement representations)

For the magnitude and sign representation the multiplication procedure must form the product of two positive factors and append the appropriate sign. The sign of the product is trivially determined from the signs of the factors, and therefore the entire foregoing argument applies directly for this representation.

For both complement representations, however, certain adjustments are necessary in the Boolean functions because the sign of the numerical data participates more intimately in the computational procedures.

For the 1's complement representation the multiplier has been rephrased as a signed magnitude, whence the entire foregoing argument becomes directly applicable when the Boolean function which affixes the signs of the b's is adjusted to accommodate the sign of the multiplier.

For the 2's complement representation the term $-x_{W-1} \cdot 2^W$ in the rephrased definition is momentarily disregarded, and the b's are determined for the integer which is defined by the remaining summation. Consequently one more coefficient b is determined than there were originally digits x, and the coefficient b_n is associated with the same power (n) of 2 as is the momentarily disregarded digit x_{W-1}. Through a slight readjustment in the Boolean function which establishes the sign of a particular one of the b's, the coefficient b_n is forced to have the same value as, and therefore to cancel, the now reconsidered digit x_{W-1}. The number of remaining b's is therefore n = W, which, indeed, is equal to the original number of digits x_i.

For all three representations, then, the same number of b's are developed.

The resulting Boolean functions are exhibited in Fig. 8. Here the b's are expressed recursively as functions of the x's for all three number representations.

From the relationships between n and W it follows that the expected numbers of non-zero b's for an arbitrary multiplier must be computed for the 2's complement representation from the previously exhibited E_j for $j = n-1$ and for the other two representations from the previously exhibited E_n.

$$X_A: \quad a_i = x_i \qquad n = W-1$$

$$X_1: \quad a_i = \left[(1 - x_i)\, x_{W-1} + (1 - x_{W-1})\, x_i\right] \qquad n = W-1$$

$$X_2: \quad a_i = x_i \qquad n = W$$

$$\left.\begin{aligned} \lambda_{j+1} &= a_j\,(\lambda_j + \gamma_{j-1}) \\ \gamma_j &= (1 - \gamma_{j-1})\left[(1 - a_j)\,\lambda_j + (1 - \lambda_j)\,a_j\right] \end{aligned}\right\} \quad j = 0, 1, \ldots W-1$$

$$\lambda_0 = \gamma_{-1} = 0.$$

$$X_A: \quad b_j = (1 - 2a_{j+1})\,\gamma_j \qquad j = 0, 1, \ldots W-1$$

$$X_1: \quad b_j = (1 - 2a_{j+1})(1 - 2x_{W-1})\,\gamma_j \qquad j = 0, 1, \ldots W-1$$

$$X_2: \quad \begin{cases} b_j = (1 - 2a_{j+1})\,\gamma_j & j = 0, 1, \ldots W-2 \\ b_{W-1} = (1 - 2a_{W-1})\,\gamma_{W-1} & \end{cases}$$

Fig. 8.

Fig. 9 exhibits the ratios of these expected numbers of non-zero replacement coefficients to the number of digits which express the signed multiplier. Clearly these ratios are very much alike and approach quite closely to 1/3 for all three representations when W assumes the value of a conventional "number length."

These are the minimum expected numbers of additions and subtractions per multiplier digit.

These expected numbers are not intended for naive interpretation.

It was earlier acknowledged that his discussion is not concerned with potential reductions in multiplication time through reducing the number of required shifts, nor through possible interplay of shifting action with adding and subtracting.

Also, the assumption of the independence of the probabilities upon which the expected numbers are based should be carefully considered. This assumption is challenged to a moderate degree by the normalization of floating-radix multipliers and by the scaling of fixed-radix multipliers to lie comfortably within the permitted range.

Yet, to the considerable extent to which the independence assumption is valid, these expected numbers express a measure of the minimum number of additions and subtractions which need be performed per multiplier digit; and to the extent to which multiplication time is determined by the number of additions and subtractions which are performed, they express a measure of the minimum time in which binary multiplication is performable.

$$E_A = 1/3 + 1/(9W) - (9 + (-1)^W)/(9W - 2^W)$$

$$E_1 = 1/3 + 1/(9W) - (9 + (-1)^W)/(9W - 2^W)$$

$$E_2 = 1/3 + 1/(9W) - (-1)^W/(9W - 2^W)$$

Fig. 9.

George W. Reitwiesner

GEORGE W. REITWIESNER